# 3

# Coset Progressions and Bohr Sets

## 3.1 Introduction

We noted in Section 1.1 that finite subgroups and small sets were trivial examples of sets of small doubling. In this chapter we present and develop some more interesting examples of sets of small doubling in abelian groups, starting with the following.

**Definition 3.1.1** (coset progression) Given elements $x_1, \dots, x_r$ of an abelian group $G$, and positive integers $L_1, \dots, L_r$, we call the set

$$P(x_1, \dots, x_r; L_1, \dots, L_r) = \{\ell_1 x_1 + \dots + \ell_r x_r : -L_i \leq \ell_i \leq L_i\}$$

a *generalised arithmetic progression*, or simply a *progression*, with *rank* $r$ and *side lengths* $L_1, \dots, L_r$. We define this progression to be *proper* if the elements $\ell_1 x_1 + \dots + \ell_r x_r$ are distinct for distinct $(\ell_1, \dots, \ell_r) \in [L_1]^{\pm} \times \dots \times [L_r]^{\pm}$. We sometimes abbreviate $P(x_1, \dots, x_d; L_1, \dots, L_d)$ as $P(x; L)$ or $P(x; L_1, \dots, L_d)$.

If, in addition, $H$ is a finite subgroup of $G$ we call the set $H + P(x; L)$ a *coset progression* of rank $r$. We define $H + P(x; L)$ to be *proper* if the elements $h + \ell_1 x_1 + \dots + \ell_r x_r$ are distinct for distinct $(h, \ell_1, \dots, \ell_r) \in H \times [L_1]^{\pm} \times \dots \times [L_r]^{\pm}$.

Note that a finite subgroup of an abelian group is a coset progression of rank 0.

A useful way of thinking of progressions is as homomorphic images of 'boxes' in $\mathbb{Z}^r$. Indeed, given elements $x_1, \dots, x_r$ of an abelian group $G$ and $L_1, \dots, L_r \in \mathbb{N}$, and writing $B = [-L_1, L_1] \times \dots \times [-L_r, L_r] \subset \mathbb{R}^r$ and $\pi : \mathbb{Z}^r \to G$ for the unique homomorphism such that $\pi(e_i) = x_i$ for each $i$, we have $P(x; L) = \pi(\mathbb{Z}^r \cap B)$. This is illustrated in Figure 3.1.



https://doi.org/10.1017/9781108652865.004 Published online by Cambridge University Press

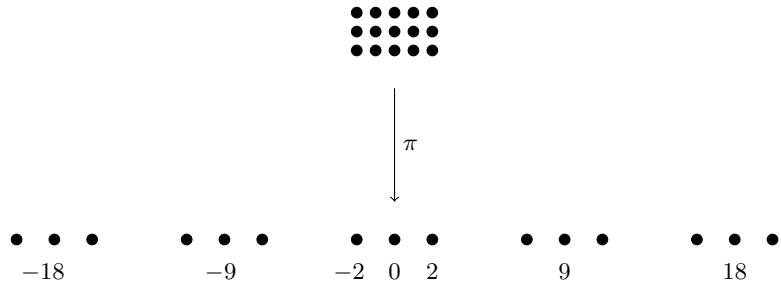


Figure 3.1 The progression $P(9,2;2,1) \subset \mathbb{Z}$ can be viewed as $\pi(\mathbb{Z}^2 \cap ([-2,2] \times [-1,1]))$, with $\pi : \mathbb{Z}^2 \to \mathbb{Z}$ defined via $\pi(1,0) = 9$ and $\pi(0,1) = 2$.

**Lemma 3.1.2** (coset progressions are approximate groups) *Let $H + P = H + P(x;L)$ be a coset progression of rank $r$ in an abelian group $G$. Let $k \in \mathbb{N}$. Then there exists a set $X \subset H + (k-1)P$ of size at most $k^r$ such that $k(H+P) \subset X + H + P$. In particular, $H + P$ is a $2^r$-approximate group, and $|k(H+P)| \leq k^r |H+P|$ for every $k \in \mathbb{N}$.*

*Proof* Let $e_1, \dots, e_r$ be the standard basis of $\mathbb{Z}^r$. Note that there exists a set $X_0 \subset (k-1)P(e;L)$ of size at most $k^r$ such that $kP(e;L) \subset X + P(e;L)$; Figure 3.2 illustrates this in the case $r = 2$, $k = 4$. Writing $\pi : \mathbb{Z}^r \to G/H$ for the unique homomorphism such that $\pi(e_i) = H + x_i$, the lemma then follows by picking, for each $x \in X_0$, an element $x' \in \pi(x)$, and taking $X$ to consist of these elements $x'$. □

It turns out that another way of producing sets of small doubling is via *inverse* images of boxes. To do this requires some notation. First, write $\mathbb{T} = \mathbb{R}/\mathbb{Z}$. Then, given $(x_1, \dots, x_d) \in \mathbb{T}^d$, define $\|(x_1, \dots, x_d)\|_{\mathbb{T}^d} \geq 0$ by writing $(\widehat{x}_1, \dots, \widehat{x}_d)$ for the unique representative of $(x_1, \dots, x_d)$ in $(-\frac{1}{2}, \frac{1}{2}]^d$, and setting $\|(x_1, \dots, x_d)\|_{\mathbb{T}^d} = \|(\widehat{x}_1, \dots, \widehat{x}_d)\|_\infty$. Write $\widehat{G}$ for the space of homomorphisms $G \to \mathbb{T}$.

**Definition 3.1.3** (Bohr set) Let $G$ be a finite abelian group, let $d \in \mathbb{N}$, let $\gamma \in \widehat{G}^d$, and let $\rho \in [0, \frac{1}{2}]$. Then we call the set

$$B(\gamma, \rho) = \{x \in G : \|\gamma(x)\|_{\mathbb{T}^d} \leq \rho\}$$

a *Bohr set* of rank $d$. In Chapter 4 it will be useful to use some alternative notation: given $\Gamma \subset \widehat{G}$ we write

$$B(\Gamma, \rho) = \{x \in G : \|\gamma(x)\|_{\mathbb{T}} \leq \rho \text{ for every } \gamma \in \Gamma\}.$$

https://doi.org/10.1017/9781108652865.004 Published online by Cambridge University Press

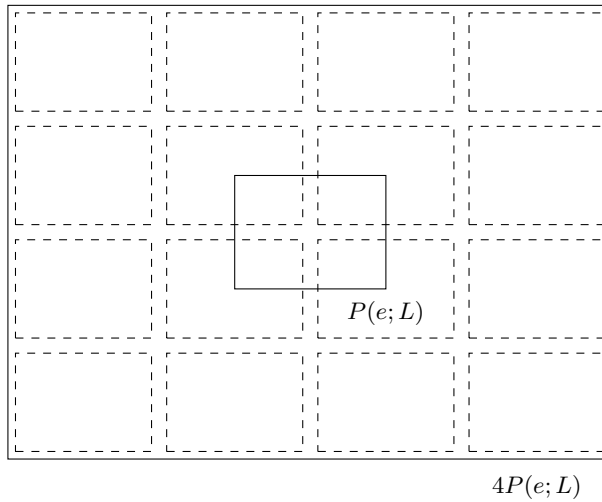


Figure 3.2 The sum set $4P(e;L)$ covered by $4^2$ translates of $P(e,L)$ in the $r=2$ case of Lemma 3.1.2.

Note that these two definitions give the same set if $\gamma = (\gamma_1, \dots, \gamma_d)$ and $\Gamma = \{\gamma_1, \dots, \gamma_d\}$.

Note that $B(\gamma, \rho)$ is the inverse image under $\gamma$ of the cube $[-\rho, \rho]^d \subset \mathbb{T}^d$.

**Proposition 3.1.4** (Bohr sets are approximate groups) *Let $G$ be an abelian group, let $d \in \mathbb{N}$, let $\gamma \in \widehat{G}^d$, and let $\rho \leq \frac{1}{2}$. Then for every $k \in \mathbb{N}$ the set $kB(\gamma,\rho)$ is covered by $(2k)^d$ translates of $B(\gamma,\rho)$. In particular, $B(\gamma,\rho)$ is a $4^d$-approximate group and $|kB(\gamma,\rho)| \leq (2k)^d |B(\gamma,\rho)|$.*

In the proof of Proposition 3.1.4 it will be helpful to define a slight variant of a Bohr set. Given $\gamma \in \widehat{G}^r$ and $\rho \leq \frac{1}{2}$, for every $\xi \in \mathbb{T}^r$ we define the *shifted Bohr set* $B(\gamma, \xi, \rho)$ via $B(\gamma,\xi,\rho) = \{x \in G : \|\gamma(x) - \xi\|_{\mathbb{T}^r} \leq \rho\}$. Thus $B(\gamma, 0, \rho) = B(\gamma, \rho)$, for example.

**Lemma 3.1.5** *Let $G$ be a finite abelian group, let $d \in \mathbb{N}$, let $\gamma \in \widehat{G}^d$, and let $\rho \leq \frac{1}{2}$. Let $\xi \in \mathbb{T}^d$. Then there exists $x_0 \in G$ such that*

$$B(\gamma, \xi, \tfrac{\rho}{2}) \subset B(\gamma,\rho) + x_0.$$

*In particular, $|B(\gamma, \xi, \frac{\rho}{2})| \leq |B(\gamma,\rho)|$.*

https://doi.org/10.1017/9781108652865.004 Published online by Cambridge University Press

*Proof* See [68, Lemma 4.20]. If $B(\gamma, \xi, \frac{\rho}{2}) = \varnothing$ then the lemma is trivial with $x_0 = 0$. If $B(\gamma, \xi, \frac{\rho}{2}) \neq \varnothing$ then pick some $x_0 \in B(\gamma, \xi, \frac{\rho}{2})$ and note that $B(\gamma, \xi, \frac{\rho}{2}) - x_0 \subset B(\gamma, \rho)$. □

*Proof of Proposition 3.1.4* Note that $kB(\gamma, \rho) \subset B(\gamma, k\rho)$. The proposition therefore follows from Lemma 3.1.5 and the fact that $B(\gamma, k\rho)$ can be covered by $(2k)^r$ sets of the form $B(\gamma, \xi, \frac{\rho}{2})$. □

We have so far identified the following sets of small doubling in abelian groups:

- sets of bounded size;
- coset progressions of bounded rank;
- Bohr sets of bounded rank.

Since these examples are all approximate groups, Lemma 2.7.4 shows that Freiman-homomorphic images of any of them are also approximate groups, and in particular sets of small doubling. Note also that, given a set of small doubling, we can always obtain further sets of small doubling simply by taking 'dense' subsets of the initial set. Indeed, given a finite set $B$ and a subset $A \subset B$, we define the *density* of $A$ in $B$ to be $|A|/|B|$. Then, if $|B^2| \leq K|B|$ and $A \subset B$ with density $1/C$, it is easy to see that $|A^2| \leq CK|A|$. Thus dense subsets of any of the examples listed above are themselves sets of small doubling. We must therefore add to the above list:

- Freiman-homomorphic images of any of the above examples;
- dense subsets of any of the above examples.

The principal aim of this chapter is to prove various results expressing the different examples in this list in terms of one another. In the next section we show that both sets of bounded size and Freiman-homomorphic images of coset progressions are dense subsets of coset progressions. In the last two sections we prove the following theorem, which is the main result of this chapter.

**Theorem 3.1.6** *Let $G$ be an abelian group. Suppose that $B_0$ is a Bohr set of rank $d$ in some finite abelian group and $\varphi : 3B_0 \to G$ is a centred Freiman 2-homomorphism, and write $B = \varphi(B_0)$. Then there exists a coset progression $H+P$ of rank at most $d+(8d)^{2d}$ such that $B \subset H+P \subset (2+(8d)^{2d})B$. In particular, by Lemmas 3.1.4 and 2.7.4, $B$ has density at least $1/\exp(\exp(O(d^{O(1)})))$ in $H+P$.*

https://doi.org/10.1017/9781108652865.004 Published online by Cambridge University Press

Thus, every example we have given so far of a set of small doubling in an abelian group can be realised as a dense subset of a coset progression. It turns out that this is a general phenomenon: in Chapter 4 we prove the *Freiman–Green–Ruzsa theorem*, Theorem 4.1.2, which states that every set of small doubling in an abelian group can be realised as a dense subset of a coset progression.

*Remark* At first sight it is somewhat unsatisfactory to have the double-exponential dependence on the rank $d$ in the bound on the density in Theorem 3.1.6. However, we should really compare the density to the *doubling constant* of $B$, which by Lemma 3.1.4 is exponential in $d$. The rank of the coset progression given by Theorem 3.1.6 is thus of comparable order to the doubling constant, and its density in $B$ is just a single exponential in the doubling constant. These bounds are comparable to the bounds that one would obtain using the more general Freiman–Green–Ruzsa theorem from the next chapter (Theorem 4.1.2).

*Remark* The reader is invited to show in Exercise 3.1 that a coset progression can always be realised as a Freiman image of a Bohr set. This can be seen as a strong converse to Theorem 3.1.6, and in conjunction with that theorem shows that Bohr sets and coset progressions are essentially equivalent notions.

## 3.2 Small Sets and Freiman Images of Coset Progressions

We can make an immediate reduction to the list of examples we gave at the end of the last section. Given a subset $A \subset G$ of size at most $K$, say $A = \{a_1, \dots, a_r\}$ with $r \leq K$, we have

$$A \subset P(a_1, \dots, a_r; 1, \dots, 1). \tag{3.2.1}$$

Thus $A$ is contained with density at most $3^K$ in a progression of rank at most $K$. We may therefore remove sets of bounded size from the list.

*Remark* 3.2.1 It is important to note that whilst (3.2.1) allows us to reduce the list of examples of sets of small doubling from a *qualitative* perspective, from a *quantitative* perspective we have lost something, since the size and doubling constant of the progression given by (3.2.1) are both exponential in the doubling constant of the set we started with. If one is concerned with optimising bounds, it can therefore be useful

https://doi.org/10.1017/9781108652865.004 Published online by Cambridge University Press

to treat small sets as being separate from coset progressions; we give further details in Remark 4.1.8.

We can also ignore Freiman-homomorphic images of coset progressions, since they are themselves dense subsets of coset progressions, as follows.

**Lemma 3.2.2** *Let $G$ be an abelian group and let $H + P$ be a coset progression of rank $r$ in some other abelian group. Suppose that $\varphi : H + P \to G$ is a Freiman 2-homomorphism. Then $\varphi(H+P)-\varphi(0)$ is also a coset progression of rank $r$. In particular, $\varphi(H+P)+\{0,-\varphi(0),-2\varphi(0)\}$ is a coset progression of rank $r+1$ containing $\varphi(H+P)$ as a subset of density at least $\frac{1}{3}$.*

*Proof* Writing $P = P(x_1, \dots, x_r; L_1, \dots, L_r)$, set $y_i = \varphi(x_i) - \varphi(0)$ for each $i = 1, \dots, r$. We claim that

$$\varphi(H + P) = \varphi(H) + P(y_1, \dots, y_r; L_1, \dots, L_r). \tag{3.2.2}$$

Since Lemma 2.7.2 (iii) and Lemma 2.7.3 (iii) imply that $\varphi(H) - \varphi(0)$ is a subgroup of $G$, this is sufficient. In fact, we prove that

$$\varphi(h + \ell_1 x_1 + \cdots + \ell_r x_r) = \varphi(h) + \ell_1 y_1 + \cdots + \ell_r y_r \tag{3.2.3}$$

whenever $h \in H$ and $|\ell_i| \le L_i$.

It follows from Lemma 2.7.2 (ii) that $-y_i = \varphi(-x_i) - \varphi(0)$. We may therefore, on replacing $x_i$ by $-x_i$ and $y_i$ by $-y_i$ where necessary, assume that $\ell_i \ge 0$ for each $i$ in (3.2.3). Moreover, (3.2.3) holds trivially when $\ell_i = 0$ for every $i$, so we may assume that $\ell_1 + \cdots + \ell_r > 0$. This implies in particular that there exists some $\ell_i > 0$, and so by induction on $\ell_1 + \cdots + \ell_r$ we may assume that

$$\begin{aligned}\varphi(h + \ell_1 x_1 + \cdots + (\ell_i - 1)x_i + \cdots + \ell_r x_r)& \\ = \varphi(h) + \ell_1 y_1 + \cdots + (\ell_i - 1)y_i + \cdots + \ell_r y_r.&\end{aligned}$$

It follows that

$$\begin{aligned}&\varphi(h + \ell_1 x_1 + \cdots + \ell_r x_r) + \varphi(0)\\ &\quad = \varphi(h + \ell_1 x_1 + \cdots + (\ell_i - 1)x_i + \cdots + \ell_r x_r) + \varphi(x_i)\\ &\quad = \varphi(h) + \ell_1 y_1 + \cdots + \ell_i y_i + \cdots + \ell_r y_r + \varphi(0),\end{aligned}$$

which implies (3.2.3) and therefore the lemma. □

https://doi.org/10.1017/9781108652865.004 Published online by Cambridge University Press

## 3.3 Lattices

We now come onto Theorem 3.1.6. Before proving it, we will need to develop our understanding of the structure of Bohr sets. Given a finite abelian group $G$ and $\gamma \in \widehat{G}^d$, the image $\gamma(G)$ is a discrete subgroup of $\mathbb{T}^d$. Given $\rho \in [0, \frac{1}{2}]$, the Bohr set $B(\gamma, \rho)$ is then the pullback under $\gamma$ of $[-\rho, \rho]^d \cap \gamma(G)$.

To study such sets we use a field called the *geometry of numbers*. In this section and the next we present a brief summary of those aspects of the geometry of numbers that we need in order to prove Theorem 3.1.6. Our treatment is based on Cassels [21], to which the reader may turn for a far more detailed account of the field.

A significant part of the geometry of numbers is concerned with interactions between *lattices* and *symmetric convex bodies* in $\mathbb{R}^d$. In this section we define lattices and introduce some of their properties; in the next we deal with symmetric convex bodies.

**Definition 3.3.1** (lattice) Let $d \in \mathbb{N}$, and let $V$ be a $d$-dimensional real vector space. A *lattice* $\Lambda \subset V$ is a group generated by a basis for $V$. Equivalently, $\Lambda$ is a lattice if there exists a basis $x_1, \dots, x_d$ for $V$ such that

$$\Lambda = \{\xi_1 x_1 + \cdots + \xi_d x_d : \xi_i \in \mathbb{Z} \text{ for each } i\}.$$

We call $x_1, \dots, x_d$ a *basis* for $\Lambda$. If $\Gamma \subset \Lambda$ is another lattice then we say that $\Gamma$ is a *sublattice* of $\Lambda$ and write $\Gamma < \Lambda$.

It is easy to see that a lattice $\Lambda \subset \mathbb{R}^d$ is *discrete*, in the sense that given an arbitrary element $v \in \Lambda$ there exists an open neighbourhood $A$ of $v$ such that $\Lambda \cap A = \{v\}$. It is also useful to note the following converse.

**Lemma 3.3.2** *Let $d \in \mathbb{N}$, and suppose that $\Lambda$ is a discrete subgroup of a $d$-dimensional real vector space $V$ such that $\operatorname{span}_{\mathbb{R}}(\Lambda) = V$. Then $\Lambda$ is a lattice in $V$.*

*Proof* If $d = 1$, assume without loss of generality that $V = \mathbb{R}$, and note that discreteness implies that there is a minimal positive element $v \in \Lambda$. It follows that $\Lambda = \langle v \rangle$, which proves the lemma in the case $d = 1$.

If $d > 1$, let $v_0 \in \Lambda$ be arbitrary, and then note that discreteness implies that there is a minimal $\lambda > 0$ such that $\lambda v_0 \in \Lambda$. Set $v = \lambda v_0$, write $W = \operatorname{span}_{\mathbb{R}}(v)$, and note that

$$\Lambda \cap W = \langle v \rangle. \tag{3.3.1}$$

https://doi.org/10.1017/9781108652865.004 Published online by Cambridge University Press

We claim that $\Lambda/(\Lambda \cap W)$ is a discrete subgroup of $V/W$. Indeed, if $x, v_1, v_2, \ldots \in \Lambda$ and $w_1, w_2, \ldots \in \Lambda \cap W$ are such that $v_n - w_n \to x$ as $n \to \infty$ then the discreteness of $\Lambda$ implies that $v_n = x + w_n$ for all large enough $n$, and hence that $v_n$ is eventually constant modulo $W$. This implies that $\Lambda/(\Lambda \cap W)$ is discrete in $V/W$. Since $\mathrm{span}_{\mathbb{R}}(\Lambda/(\Lambda \cap W)) = V/W$, by induction we may conclude that $\Lambda/(\Lambda \cap W)$ is a lattice in $V/W$, which is to say generated by a basis for $V/W$. Adding $v$ to this basis gives a basis for $V$, which by (3.3.1) is also a generating set for $\Lambda$, which completes the proof. □

The relevance of lattices to Theorem 3.1.6 arises thanks to the following lemma.

**Lemma 3.3.3** *Let $G$ be a finite abelian group, let $\gamma \in \widehat{G}^d$, and set $\Lambda = \gamma(G) + \mathbb{Z}^d \subset \mathbb{R}^d$. Then $\Lambda$ is a lattice in $\mathbb{R}^d$.*

*Proof* Set $B = [0,1)^d$, and note that $B$ is a complete set of coset representatives for $\mathbb{Z}^d$ in $\mathbb{R}^d$. In particular, $\Lambda \cap B$ is a complete set of coset representatives for $\mathbb{Z}^d$ in $\Lambda$. Since $\mathbb{Z}^d$ has finite index (at most $|G|$) in $\Lambda$, this implies that $|\Lambda \cap B| < \infty$, from which it easily follows that $\Lambda$ is discrete. Since $\Lambda$ contains $\mathbb{Z}^d$ we have $\mathrm{span}_{\mathbb{R}}(\Lambda) = \mathbb{R}^d$, and so it follows from Lemma 3.3.2 that $\Lambda$ is a lattice, as required. □

Let $\Lambda$ be a lattice in $\mathbb{R}^d$ with basis $x_1, \ldots, x_d$, and consider the parallelopiped

$$P = \{\eta_1 x_1 + \cdots + \eta_d x_d : \eta_i \in [0,1) \text{ for each } i\}.$$

We call $P$ the *fundamental parallelopiped* for $\Lambda$ with respect to the basis $x_1, \ldots, x_d$. Since $x_1, \ldots, x_d$ is by definition also a basis for $\mathbb{R}^d$, there exist unique functions $x : \mathbb{R}^d \to \Lambda$ and $p : \mathbb{R}^d \to P$ such that

$$v = x(v) + p(v) \tag{3.3.2}$$

for each $v \in \mathbb{R}^d$. In particular, $\mathbb{R}^d$ is the countable disjoint union of the sets $x + P$ with $x \in \Lambda$.

Write vol for Lebesgue measure normalised with respect to the standard basis of $\mathbb{R}^d$. Given elements $x_1, \ldots, x_d \in \mathbb{R}^d$, define the *determinant* $\det(x_1, \ldots, x_d)$ to be the determinant of the $d \times d$ matrix whose columns are the elements $x_1, \ldots, x_d$ expressed as column vectors with respect to the standard basis for $\mathbb{R}^d$. Note that if $P$ is a fundamental parallelopiped for a lattice $\Lambda$ with respect to a basis $x_1, \ldots, x_d$ then

$$\mathrm{vol}(P) = |\det(x_1, \ldots, x_d)|. \tag{3.3.3}$$

https://doi.org/10.1017/9781108652865.004 Published online by Cambridge University Press

**Proposition 3.3.4** *Let $\Lambda$ be a lattice in $\mathbb{R}^d$ with basis $x_1, \dots, x_d$, and $\Gamma$ a sublattice with basis $y_1, \dots, y_d$. Then*

$$\frac{|\det(y_1, \dots, y_d)|}{|\det(x_1, \dots, x_d)|} = [\Lambda : \Gamma].$$

Note that Proposition 3.3.4 implies in particular that if $x_1, \dots, x_d$ and $y_1, \dots, y_d$ are two bases of the same lattice $\Lambda$ then $|\det(x_1, \dots, x_d)| = |\det(y_1, \dots, y_d)|$. Once we have proved the proposition , we may therefore define the *determinant* $\det(\Lambda)$ of a lattice $\Lambda$ by setting $\det(\Lambda) = |\det(x_1, \dots, x_d)|$ for an arbitrary basis $x_1, \dots, x_d$ of $\Lambda$.

*Proof* Let $P$ be a fundamental parallelopiped for $\Lambda$ with respect to $x_1, \dots, x_d$, and $Q$ a fundamental parallelopiped for $\Gamma$ with respect to $y_1, \dots, y_d$. Let

$$\begin{aligned} x &: \mathbb{R}^d \to \Lambda \qquad & p &: \mathbb{R}^d \to P \\ y &: \mathbb{R}^d \to \Gamma \qquad & q &: \mathbb{R}^d \to Q \end{aligned}$$

be the unique functions satisfying

$$v = x(v) + p(v) = y(v) + q(v) \tag{3.3.4}$$

for each $v \in \mathbb{R}^d$ as in (3.3.2). We claim that

$$|p^{-1}(u) \cap Q| = [\Lambda : \Gamma] \tag{3.3.5}$$

for every $u \in P$. Since $p$ is a translation on each set $x + P$ with $x \in \Lambda$, it is measure preserving on restriction to each such set, and so (3.3.5) will then imply that $p(Q) = P$ and $\mathrm{vol}(Q) = [\Lambda : \Gamma] \mathrm{vol}(P)$, which by (3.3.3) gives the desired result.

To prove (3.3.5), first note that the uniqueness of $y(v)$ and $q(v)$ in (3.3.4) implies that $Q$ is a complete set of coset representatives for $\Gamma$ in $\mathbb{R}^d$. It follows that for every $u \in \mathbb{R}^d$ the set $Q - u$ is also a complete set of coset representatives for $\Gamma$ in $\mathbb{R}^d$. This implies that for every $u \in \mathbb{R}^d$ the set $\Lambda \cap (Q - u)$ is a complete set of coset representatives for $\Gamma$ in $\Lambda$. This in turn implies in particular that $|\Lambda \cap (Q - u)| = [\Lambda : \Gamma]$, and hence that $|(\Lambda + u) \cap Q| = [\Lambda : \Gamma]$. However, if $u \in P$ then $(\Lambda + u) \cap Q$ is precisely $|p^{-1}(u) \cap Q|$, and so this gives (3.3.5), as claimed. □

https://doi.org/10.1017/9781108652865.004 Published online by Cambridge University Press

A similar argument to the proof of Proposition 3.3.4 gives the following.

**Lemma 3.3.5** (Blichfeldt [7]) *Let $d \in \mathbb{N}$. Let $\Lambda$ be a lattice in $\mathbb{R}^d$, and let $A \subset \mathbb{R}^d$ be a measurable set. Suppose that*

$$(A - A) \cap \Lambda = \{0\}. \tag{3.3.6}$$

*Then* $\mathrm{vol}(A) \leq \det(\Lambda)$.

*Proof* Let $x_1, \ldots, x_d$ be a basis for $\Lambda$, write $P$ for the corresponding fundamental parallelopiped, and define maps $x : \mathbb{R}^d \to \Lambda$ and $p : \mathbb{R}^d \to P$ as in (3.3.2). On restriction to each set of the form $x + P$ with $x \in \Lambda$ the map $p$ is a translation, and hence measure preserving. Moreover, (3.3.6) implies that for every $u \in P$ we have $|p^{-1}(u) \cap A| \leq 1$. It follows that $\mathrm{vol}(A) \leq \mathrm{vol}(p(A)) \leq \mathrm{vol}(P) = |\det(x_1, \ldots, x_d)|$, as required. □

## 3.4 Convex Bodies

In studying the Bohr set $B(\gamma, \rho)$ we essentially study the interaction of the lattice coming from Lemma 3.3.3 with the cube $[-\rho, \rho]$. The only property of $[-\rho, \rho]$ that we will really need is that its interior, $(-\rho, \rho)$, is a so-called *symmetric convex body*. We now define this term, starting with the adjective *convex*.

**Definition 3.4.1** (convex set) Let $V$ be a finite-dimensional real vector space. A set $A \subset V$ is said to be *convex* if whenever $x, y \in A$ and $\rho \in (0, 1)$ the point $\rho x + (1 - \rho)y \in A$ as well.

**Definition 3.4.2** (convex body) A *convex body* $B \subset \mathbb{R}^d$ is a non-empty bounded open convex set; it is *symmetric* if for every $x \in B$ we also have $-x \in B$.

The purpose of this short section is to record some elementary properties of convex bodies. We start by introducing and clarifying some notation. Throughout the rest of this chapter, whenever $A \subset \mathbb{R}^d$ and $\lambda \in \mathbb{R}$, we write $\lambda A$ for the *dilate*

$$\lambda A = \{\lambda a : a \in A\}.$$

Note that if $\lambda \in \mathbb{Z}$ then there is the potential for ambiguity here, since in general we have defined $\lambda A$ to be the iterated sum set $A + \cdots + A$.

https://doi.org/10.1017/9781108652865.004 Published online by Cambridge University Press

When there is the danger of this, we write instead

$$\lambda \cdot A = \{\lambda a : a \in A\}$$

to distinguish the dilate from the iterated sum set.

The following lemma shows that in the setting of symmetric convex bodies this potential ambiguity is harmless.

**Lemma 3.4.3** *Let $d \in \mathbb{N}$ and let $B \subset \mathbb{R}^d$ be a symmetric convex body. Then for every $k, \ell \in \mathbb{N}$ we have*

$$k \cdot B - \ell \cdot B = kB - \ell B = (k + \ell)B.$$

The proof of Lemma 3.4.3 is a straightforward exercise, and so we omit it. The same goes for the following lemma.

**Lemma 3.4.4** *Let $d, k \in \mathbb{N}$. Suppose $B \subset \mathbb{R}^d$ is a convex body and $\pi : \mathbb{R}^d \to \mathbb{R}^k$ is a linear map. Then $\pi(B)$ is also a convex body, and if $B$ is symmetric then so is $\pi(B)$.*

**Lemma 3.4.5** *Let $d \in \mathbb{N}$. Suppose that $U, V < \mathbb{R}^d$ are complementary subspaces, in the sense that $\mathbb{R}^d = U \oplus V$, and write $\pi : \mathbb{R}^d \to V$ for the projection taking $(u, v) \in U \oplus V = \mathbb{R}^d$ to $u \in U$. Suppose $B \subset \mathbb{R}^d$ is a convex body. Then there is a continuous map $f : \pi(B) \to B$ that is a right inverse to $\pi$ in the sense that $\pi \circ f$ is the identity on $\pi(B)$.*

*Proof* Set $k = \dim V$. We first prove the lemma in the case where $k = 1$, say $V = \mathrm{span}_{\mathbb{R}}(v_0)$ for some $v_0 \in \mathbb{R}^d$. Define functions $\varphi^+, \varphi^- : \pi(B) \to \mathbb{R}$ by setting

$$\varphi^+(u) = \sup\{\lambda \in \mathbb{R} : u + \lambda v_0 \in B\},$$
$$\varphi^-(u) = \inf\{\lambda \in \mathbb{R} : u + \lambda v_0 \in B\}.$$

We claim first that $\varphi^+$ and $\varphi^-$ are continuous. Let $u \in \pi(B)$, noting that by definition there exists $\xi \in \mathbb{R}$ such that $u + \xi v_0 \in B$. The openness of $B$ therefore implies that there exists an open neighbourhood $N$ of $u$ in $U$ such that

$$u + N + \xi v_0 \subset B. \tag{3.4.1}$$

It then follows from (3.4.1), convexity and the definition of $\varphi^+$ that for every $\varepsilon \in (0, 1)$ and every $x \in \mathbb{N}$ we have

$$\varphi^+(u + \varepsilon x) \in \varphi^+(u) + [-\varepsilon(\varphi^+(u) - \xi), \varepsilon(\varphi^+(u) - \xi)],$$

and so $\varphi^+$ is continuous at $u$, as claimed. The proof that $\varphi^-$ is continuous

https://doi.org/10.1017/9781108652865.004 Published online by Cambridge University Press

is essentially identical (alternatively, replacing $v_0$ by $-v_0$ puts $-\varphi^-$ in the role of $\varphi^+$).

Given $u \in \pi(B)$, it follows from convexity and the definitions of $\varphi^+$ and $\varphi^-$ that

$$v + \tfrac{1}{2}(\varphi^+(u) + \varphi^-(u))v_0 \in B.$$

This implies we may define a function $f : \pi(B) \to B$ by $f(u) = \frac{1}{2}(\varphi^+(u) + \varphi^-(u))v_0$. This is trivially a right inverse to $\pi$, and is continuous by the continuity of $\varphi^+$ and $\varphi^-$, and so satisfies the requirements of the lemma in the case $k = 1$.

If $k > 1$, let $v_1, \dots, v_k$ be a basis for $V$. For each $j = 1, \dots, k$ set $V_j = \mathrm{span}_{\mathbb{R}}(v_j)$ and $U_j = \mathrm{span}_{\mathbb{R}}(v_{j+1}, \dots, v_k) + U$, and define $\pi_j : V_j \oplus U_j \to U_j$ by setting

$$\pi_j(\lambda_j v_j + \cdots + \lambda_k v_k + u) = \lambda_{j+1} v_{j+1} + \cdots + \lambda_k v_k + u$$

for every $\lambda_i \in \mathbb{R}$ and $u \in U$. By repeated application of Lemma 3.4.4, for each $j$ the set $\pi_j \circ \cdots \circ \pi_1(B)$ is a convex body in $U_j$. By the case $k = 1$ of the lemma, for each $j$ we may therefore define a continuous function

$$f_j : \pi_j \circ \cdots \circ \pi_1(B) \to \pi_{j-1} \circ \cdots \circ \pi_1(B)$$

that is a right inverse to $\pi_j$. Since

$$\pi = \pi_k \circ \cdots \circ \pi_1,$$

the function

$$f_1 \circ \cdots \circ f_k : \pi(B) \to B$$

is therefore a continuous right inverse to $\pi$, and so satisfies the requirements of the lemma. □

## 3.5 Successive Minima and Minkowski's Second Theorem

Given a symmetric convex body $B \subset \mathbb{R}^d$, we define the *successive minima* $\lambda_1, \dots, \lambda_d$ of $B$ with respect to $\Lambda$ via

$$\lambda_i = \inf\{\lambda > 0 : \dim \mathrm{span}_{\mathbb{R}}(\lambda B \cap \Lambda) \geq i\}.$$

Writing $\overline{B}$ for the closure of $B$, we may choose inductively a list

$$v_1, \dots, v_d \in \mathbb{Z}^d$$

https://doi.org/10.1017/9781108652865.004 Published online by Cambridge University Press

of linearly independent vectors such that $v_1, \dots, v_i \in \lambda_i \overline{B}$ for every $i$. We call such a list a *directional basis* for $\Lambda$ with respect to $B$; note that for a given $B$ and $\Lambda$, a directional basis may not be uniquely defined. We also caution that a directional basis for $\Lambda$ with respect to $B$ need not be a basis for $\Lambda$ in the sense of Definition 3.3.1 (see Exercise 3.5).

The key result we will need from the geometry of numbers is the following.

**Theorem 3.5.1** (Minkowski's second theorem) *Let $B \subset \mathbb{R}^d$ be a symmetric convex body and let $\Lambda$ be a lattice. Write $\lambda_1 \leq \cdots \leq \lambda_d$ for the successive minima of $B$ with respect to $\Lambda$. Then $\lambda_1 \dots \lambda_d \operatorname{vol}(B) \leq 2^d \det(\Lambda)$.*

Minkowski's second theorem actually also includes the lower bound $\lambda_1 \cdots \lambda_d \operatorname{vol}(B) \geq \frac{2^n}{n!} \det(\Lambda)$, but in this book we need only the upper bound stated in Theorem 3.5.1. The reader interested in the lower bound can consult [21, §VIII.4.3] for a proof.

We prove Theorem 3.5.1 following Tao and Vu [68, §3.5], starting with a result they call the *squeezing lemma*.

**Lemma 3.5.2** (squeezing lemma [68, Lemma 3.31]) *Let $d, k \in \mathbb{N}$, let $\mu \in (0, 1]$, let $B \subset \mathbb{R}^d$ be a convex body, and let $V < \mathbb{R}^d$ be a $k$-dimensional subspace. Suppose that $A \subset B$ is an open set. Then there exists an open subset $A' \subset B$ satisfying*

$$\operatorname{vol}(A') = \mu^k \operatorname{vol}(A) \tag{3.5.1}$$

*and*

$$(A' - A') \cap V \subset (\mu(A - A)) \cap V. \tag{3.5.2}$$

*Proof* Let $U$ be a complementary subspace to $V$ in $\mathbb{R}^d$, so that $\mathbb{R}^d = U \oplus V$. Define the projection $\pi : \mathbb{R}^d \to U$ by setting $\pi(u + v) = u$ for every $u \in U$ and $v \in V$.

Let $f : \pi(B) \to B$ be the continuous right inverse to $\pi$ given by Lemma 3.4.5, and note that by the convexity of $B$ we may set

$$\begin{array}{rccc} \Phi & : & B & \to & B \\ & & x & \mapsto & \mu x + (1 - \mu) f(\pi(x)). \end{array}$$

We claim that $\Phi$ is a homeomorphism from $B$ to $\Phi(B)$. It is certainly continuous by the continuity of $f$ and $\pi$; we will show that it has a continuous inverse $\Phi(B) \to B$. First note that, by definition of $f$, there exists a continuous map $\varphi : \pi(B) \to V$ such that $f(u) = u + \varphi(u)$ for

https://doi.org/10.1017/9781108652865.004 Published online by Cambridge University Press

every $u \in \pi(B)$. For every $u \in U$ and $v \in V$ with $u + v \in B$, it follows that

$$\Phi(u + v) = u + \varphi(u) + \mu(v - \varphi(u)). \tag{3.5.3}$$

It follows that the map $\Phi(B) \to B$ defined by $u+v \mapsto u+\varphi(u)+\mu^{-1}(v-\varphi(u))$ is an inverse to $\Phi$. The continuity of $\varphi$ ensures that this inverse is continuous, and so $\Phi$ is a homeomorphism, as required.

The set $A' = \Phi(A)$ is therefore open. It is also a subset of $B$ by definition of $\Phi$. The expression (3.5.3) for $\Phi$ shows that for each $u \in U$ the map $\Phi$ contracts the set $A \cap (u+V)$ by a factor of $\mu$ in every direction of $V$, so Fubini's theorem (Theorem 1.5.4) gives (3.5.1).

Finally, suppose that $y \in (A' - A') \cap V$. By definition there exist $x_1, x_2 \in A$ such that $y = \Phi(x_1) - \Phi(x_2)$. Writing each $x_i$ in the form $x_i = u_i + v_i$ for some $u_i \in U$ and $v_i \in V$, we may conclude from (3.5.3) that

$$y = u_1 - u_2 + \varphi(u_1) - \varphi(u_2) + \mu(v_1 - v_2 - \varphi(u_1) + \varphi(u_2)). \tag{3.5.4}$$

However, the assumption that $y \in V$ then forces $u_1 = u_2$, which combined with (3.5.4) implies that

$$\begin{aligned} y &= \mu(v_1 - v_2) \\ &= \mu(x_1 - x_2) \\ &\in \mu(A - A), \end{aligned}$$

giving (3.5.2), as required. □

*Proof of Theorem 3.5.1* We follow Tao and Vu [68, §3.5]. Fix a directional basis $v_1, \dots, v_d$ for $\Lambda$ with respect to $B$, and for each $i = 0, 1, \dots, d$ set $V_i = \operatorname{span}_{\mathbb{R}}(v_1, \dots, v_i)$ and $\Lambda_i = \Lambda \cap (V_i \setminus V_{i-1})$, noting that

$$\lambda_j B \cap \Lambda_j = \{0\} \tag{3.5.5}$$

by definition of $\lambda_j$ and $\Lambda_j$.

Set $B_0 = \frac{\lambda_d}{2} B$. Starting with $A_0 = B_0$, apply Lemma 3.5.2 iteratively to obtain a sequence $A_0, A_1, \dots, A_{d-1}$ of open subsets of the convex body $B_0$ such that

$$\operatorname{vol}(A_i) = \left(\frac{\lambda_i}{\lambda_{i+1}}\right)^j \operatorname{vol}(A_{i-1}) \tag{3.5.6}$$

and

$$(A_i - A_i) \cap V_i \subset \left(\frac{\lambda_i}{\lambda_{i+1}}(A_{i-1} - A_{j-1})\right) \cap V \tag{3.5.7}$$

https://doi.org/10.1017/9781108652865.004 Published online by Cambridge University Press

for each $i$.

It is immediate from (3.5.6) and the definition of $A_0$ that

$$\mathrm{vol}(A_{d-1}) = \frac{\lambda_1 \dots \lambda_d \,\mathrm{vol}(B)}{2^d}. \tag{3.5.8}$$

For each $j$ we have

$$\begin{aligned}
(A_{d-1} - A_{d-1}) \cap V_j &\subset \left(\tfrac{\lambda_j}{\lambda_d}(A_{j-1} - A_{j-1})\right) \cap V_j && \text{(by (3.5.7))}\\
&\subset \left(\tfrac{\lambda_j}{\lambda_d}(B_0 - B_0)\right) \cap V_j && \text{(since } A_{j-1} \subset B_0\text{)}\\
&\subset \left(\tfrac{\lambda_j}{\lambda_d}\left(\tfrac{\lambda_d}{2}B - \tfrac{\lambda_d}{2}B\right)\right) \cap V_j && \text{(by definition of } B_0\text{)}\\
&\subset (\lambda_j B) \cap V_j && \text{(by Lemma 3.4.3),}
\end{aligned}$$

which by (3.5.5) and the definition of $\Lambda_j$ implies that $(A_{d-1} - A_{d-1}) \cap \Lambda_j = \{0\}$. Since this holds for all $j$, we conclude that

$$(A_{d-1} - A_{d-1}) \cap \Lambda = \{0\}.$$

Lemma 3.3.5 therefore combines with (3.5.8) to prove the theorem. □

## 3.6 Finding Dense Coset Progressions in Bohr Sets

In this section we prove Theorem 3.1.6. Slightly counterintuitively, the main step is to show that a Bohr set *contains* a progression as a dense subset, as follows.

**Proposition 3.6.1** *Let $G$ be a finite abelian group, let $d \in \mathbb{N}$, let $\gamma \in \widehat{G}^d$, and let $\rho \in (0, \frac{1}{6})$. Then $B(\gamma, \rho)$ contains a proper coset progression $H + P$ of rank at most $d$ and size at least $|B(\gamma, \rho)|/(4d)^{2d}$.*

Once we have this, Ruzsa's covering argument allows us to obtain the desired containment in the opposite direction, as follows.

*Proof of Theorem 3.1.6* It follows from Proposition 3.6.1 that $B_0$ contains a coset progression $H_0 + P_0$ of rank at most $d$ and size at least $|B_0|/(4d)^{2d}$. Proposition 3.1.4 implies that $|B_0 + H_0 + P_0| \leq 4^d |B_0|$, which means in particular that $|B_0 + H_0 + P_0| \leq (8d)^{2d} |H_0 + P_0|$. Lemma 2.4.4 then implies that there exists a set $X \subset B_0$ of size at most $(8d)^{2d}$ such that $B_0 \subset X + (H_0 + P_0) - (H_0 + P_0)$, and hence

$$B \subset \varphi(X) + \varphi(H_0 + P_0) - \varphi(H_0 + P_0). \tag{3.6.1}$$

https://doi.org/10.1017/9781108652865.004 Published online by Cambridge University Press

Since $\varphi$ is centred, Lemma 3.2.2 implies that there exists a coset progression $H + P \subset G$ of rank at most $d$ such that $\varphi(H_0 + P_0) = H + P$, and the inclusion (3.6.1) therefore becomes $B \subset \varphi(X) + H + 2P$. However, writing $\varphi(X) = \{x_1, \dots, x_t\}$, and defining $P' = P(x_1, \dots, x_t; 1, \dots, 1)$ in a similar fashion to (3.2.1), we have $\varphi(X) \subset P'$, and hence

$$B \subset H + 2P + P' \subset \left(2 + (8d)^{2d}\right) B$$

by Lemma 2.7.2 (ii). Since $H + 2P + P'$ is a coset progression of rank at most $d + (8d)^{2d}$, the theorem is proved. □

Proposition 3.6.1 is immediate from the following two propositions.

**Proposition 3.6.2** *Let $G$ be a finite abelian group, let $d \in \mathbb{N}$, let $\gamma \in \widehat{G}^d$, and let $\rho \in (0, \frac{1}{2})$. Let $\Lambda$ be the pullback to $\mathbb{R}^d$ of the subgroup $\gamma(G)$ of $\mathbb{R}^d/\mathbb{Z}^d$, and write $\lambda_1, \dots, \lambda_d$ for the successive minima of the cube $Q = (-1, 1)^d$ with respect to $\Lambda$. Define $r = \dim \operatorname{span}_{\mathbb{R}}(\Lambda \cap \rho\overline{Q})$. Then $B(\gamma, \rho)$ contains a proper coset progression $H + P$ of rank $r$ and size at least $(\rho/r)^r \lambda_{r+1} \cdots \lambda_d |G|$. In particular, $H + P$ has rank at most $d$ and size at least $(\rho/d)^d |G|$.*

**Proposition 3.6.3** *Let $G$ be a finite abelian group, let $d \in \mathbb{N}$, let $\gamma \in \widehat{G}^d$, and let $\rho \in (0, \frac{1}{6})$. Let $\Lambda$ be the pullback to $\mathbb{R}^d$ of the subgroup $\gamma(G)$ of $\mathbb{R}^d/\mathbb{Z}^d$, and write $\lambda_1, \dots, \lambda_d$ for the successive minima of the cube $Q = (-1, 1)^d$ with respect to $\Lambda$. Define $r = \dim \operatorname{span}_{\mathbb{R}}(\Lambda \cap \rho\overline{Q})$. Then we have*

$$|B(\gamma, \rho)| \leq (12d)^d \rho^r \lambda_{r+1} \cdots \lambda_d |G|.$$

*Proof of Proposition 3.6.2* Let $v_1, \dots, v_d$ be a directional basis for $\Lambda$ with respect to $Q$, and for $i = 1, \dots, r$ write $L_i = \rho/(r\lambda_i)$. Note that

$$P(v_1, \dots, v_r; L_1, \dots, L_r) \subset \rho\overline{Q} \cap \Lambda. \tag{3.6.2}$$

Set $H = \ker \gamma$, pick an arbitrary $x_i \in G$ such that $\gamma(x_i) \equiv v_i \pmod{\mathbb{Z}^d}$ for each $i \in [r]$, and set

$$P = P(x_1, \dots, x_r; L_1, \dots, L_r),$$

noting that $H + P \subset B(\gamma, \rho)$. We claim that $H + P$ is proper. Indeed, let $\ell_1, \dots, \ell_r, \ell_1', \dots, \ell_r'$ with $|\ell_i| \leq L_i$ be such that

$$\ell_1 x_1 + \cdots + \ell_r x_r \in \ell_1' x_1 + \cdots + \ell_r' x_r + H.$$

By (3.6.2) we then have

$$(\ell_1 - \ell_1')v_1 + \cdots + (\ell_r - \ell_r')v_r \in 2\rho\overline{Q} \cap \mathbb{Z}^d,$$

https://doi.org/10.1017/9781108652865.004 Published online by Cambridge University Press

which by the linear independence of the $v_i$ and the fact that $\rho < \frac{1}{2}$ implies that $\ell_i = \ell_i'$ for every $i$, and so $H + P$ is proper as claimed.

Now note that $\det(\Lambda) = |H|/|G|$ and $\mathrm{vol}(Q) = 2^d$, so that Minkowski's second theorem (Theorem 3.5.1) gives

$$\lambda_1 \cdots \lambda_d \leq \frac{|H|}{|G|}. \tag{3.6.3}$$

We therefore have

$$\begin{aligned} |H + P| &\geq L_1 \cdots L_r |H| && \text{(by properness)} \\ &= \frac{\rho^r |H|}{r^r \lambda_1 \cdots \lambda_r} \\ &\geq (\rho/r)^r \lambda_{r+1} \cdots \lambda_d |G| && \text{(by (3.6.3))}, \end{aligned}$$

and so $H + P$ is of the required size and the proof is complete. □

In proving Proposition 3.6.3 it will be convenient to define, for a given symmetric convex body $B \subset \mathbb{R}^d$, the norm $\|\cdot\|_B$ on $\mathbb{R}^d$ via $\|x\|_B = \inf\{\nu \geq 0 : x \in \nu B\}$. It turns out that $\|\cdot\|_B$ is indeed a norm. However, as we will not need this fact we leave it to the reader to prove it in Exercise 3.6, along with the converse statement that the unit ball of an arbitrary norm on $\mathbb{R}^d$ is a symmetric convex body.

**Lemma 3.6.4** *Let $B$ be a symmetric convex body in $\mathbb{R}^d$ and let $\Lambda$ be a lattice in $\mathbb{R}^d$. Let $\lambda_1, \ldots, \lambda_d$ be the successive minima of $B$ with respect to $\Lambda$, and define $r = \dim \mathrm{span}_{\mathbb{R}}(\Lambda \cap \overline{B})$. Then there exists a basis $x_1, \ldots, x_d$ for $\mathbb{R}^d$ with $x_i \in \Lambda$ for each $i$ such that $1 < \|x_i\|_B \leq 2$ for $i = 1, \ldots, r$ and $\|x_i\|_B = \lambda_i$ for $i = r+1, \ldots, d$, and such that $\overline{B} \cap \langle x_1, \ldots, x_d \rangle = \{0\}$.*

*Proof* Let $v_1, \ldots, v_d$ be a directional basis for $\Lambda$ with respect to $B$. For $i = d, \ldots, 1$ in turn, define

$$\alpha_i = \min\{\alpha \in \mathbb{N} : \|\alpha \alpha_{i+1} \cdots \alpha_d v_i\|_B > 1\},$$

noting that

$$\alpha_k \cdots \alpha_d > \lambda_k^{-1} \tag{3.6.4}$$

for every $k$. Set $x_i = \alpha_i \cdots \alpha_d v_i$ for each $i$, noting that $1 < \|x_i\|_B \leq 2$ for $i = 1, \ldots, r$ and $\|x_i\| = \lambda_i$ for $i = r+1, \ldots, d$, as required.

It remains to show that $\overline{B} \cap \langle x_1, \ldots, x_d \rangle = \{0\}$. To that end, let $y \in \overline{B} \cap \langle x_1, \ldots, x_d \rangle$, and let $k$ be minimal such that $y \in \mathrm{span}_{\mathbb{R}}(v_1, \ldots, v_k)$. This implies that $y \in \langle x_1, \ldots, x_k \rangle$, and hence $y \in \alpha_k \cdots \alpha_d \langle v_1, \ldots, v_k \rangle$.

https://doi.org/10.1017/9781108652865.004 Published online by Cambridge University Press

It follows that

$$\frac{y}{\alpha_k \cdots \alpha_d} \in \left(\frac{1}{\alpha_k \cdots \alpha_d}\overline{B}\right) \cap \Lambda,$$

and hence by (3.6.4) that

$$\frac{y}{\alpha_k \cdots \alpha_d} \in \lambda_k B \cap \Lambda.$$

By the minimality of $k$ and the definitions of $\lambda_k$ and $v_k$ it follows that $y = 0$. We therefore have $\overline{B} \cap \langle x_1, \dots, x_d\rangle = \{0\}$, as required. □

*Proof of Proposition 3.6.3* Write $H = \ker \gamma$, and note that

$$|\rho\overline{Q} \cap \Lambda||H| = |B(\gamma, \rho)| \tag{3.6.5}$$

and

$$|\tfrac{1}{2}Q \cap \Lambda||H| \leq |G|. \tag{3.6.6}$$

Let $x_1, \dots, x_d \in \Lambda$ be the basis for $\mathbb{R}^d$ arising on applying Lemma 3.6.4 with $B = 2\rho Q$, noting that the successive minima of $2\rho Q$ with respect to $\Lambda$ are $\lambda_i/2\rho$. Note in particular that

$$2\rho\overline{Q} \cap \langle x_1, \dots, x_d\rangle = \{0\}. \tag{3.6.7}$$

Since $\|\cdot\|_\infty = 2\rho\|\cdot\|_B$, we have $\|x_i\|_\infty \leq 4\rho$ for $i = 1, \dots, r$ and $\|x_i\|_\infty = \lambda_i$ for $i = r+1, \dots, d$. Defining $L_i = \lfloor 1/(12d\rho)\rfloor$ for $i = 1, \dots, r$, and $L_i = \lfloor 1/(3d\lambda_i)\rfloor$ for $i = r+1, \dots, d$, it follows that $P(x; L) \subset \frac{1}{3}\overline{Q}$, and hence, since $\rho < \frac{1}{6}$, that

$$P(x; L) + \rho\overline{Q} \subset \tfrac{1}{2}Q. \tag{3.6.8}$$

Note that we have, slightly crudely,

$$|P(x; L)| \geq \frac{1}{(12d)^d \rho^r \lambda_{r+1} \cdots \lambda_d}. \tag{3.6.9}$$

Now, given two distinct elements $u, v \in P(x; L)$, we have $(u + \rho\overline{Q}) \cap (v + \rho\overline{Q}) = \varnothing$, since if $(u + \rho\overline{Q}) \cap (v + \rho\overline{Q}) \neq \varnothing$ for $u, v \in P(x; L)$ then $u - v \in 2\rho\overline{Q} \cap \langle x_1, \dots, x_d\rangle$ and then $u = v$ by (3.6.7). It therefore follows from (3.6.8) that $|\frac{1}{2}Q \cap \Lambda| \geq |P(x; L)||\rho\overline{Q} \cap \Lambda|$, and hence

$$\begin{aligned} |G| &\geq |P(x; L)||\rho\overline{Q} \cap \Lambda||H| && \text{(by (3.6.6))} \\ &\geq \frac{1}{(12d)^d \rho^r \lambda_{r+1} \cdots \lambda_d}|B(\gamma, \rho)| && \text{(by (3.6.5) and (3.6.9)),} \end{aligned}$$

and the proposition is proved. □

https://doi.org/10.1017/9781108652865.004 Published online by Cambridge University Press

## Exercises

3.1 Show that a coset progression of rank $r$ in an arbitrary abelian group is a Freiman-homomorphic image of a Bohr set of rank $r$ in some finite abelian group.

3.2 It follows from Proposition 3.6.2 that a Bohr set $B(\gamma, \rho)$ of rank $d$ inside a finite abelian group $G$ satisfies $|B(\gamma, \rho)| \geq (\rho/d)^d |G|$. Prove directly that in fact $|B(\gamma, \rho)| \geq \rho^d |G|$.

3.3 Let $G$ be an abelian group, let $\pi : \mathbb{Z}^d \to G$ be a homomorphism, and let $B \subset \mathbb{R}^d$ be a symmetric convex body. Show that the set $\pi(B \cap \mathbb{Z}^d)$ is a $K$-approximate group for some $K$ depending only on $d$. Noting that a progression is a special case of such a set in which $B$ is a cuboid, formulate a similar generalisation of a Bohr set of rank $d$, and prove that it is a $K$-approximate group with $K$ depending only on $d$.

3.4 Show that two bases $x_1, \dots, x_d$ and $y_1, \dots, y_d$ of $\mathbb{R}^d$ generate the same lattice $\Lambda$ if and only if there exists an $n \times n$ matrix $A = (a_{ij})$ with integer entries and $\det(A) = \pm 1$ such that $y_i = \sum_{j=1}^n a_{ij} x_j$ for every $i$. Use this to give an alternative proof of the fact that $\det(\Lambda)$ is well defined.

3.5 Give an example, for some $d$, of a symmetric convex body $B \subset \mathbb{R}^d$ and a lattice $\Lambda \subset \mathbb{R}^d$ such that whenever $v_1, \dots, v_d$ is a directional basis for $\Lambda$ with respect to $B$ we have $\langle v_1, \dots, v_d \rangle \neq \Lambda$. What is the smallest $d$ for which this is possible?

3.6 Show that if $B \subset \mathbb{R}^d$ is a symmetric convex body then $\| \cdot \|_B$ is a norm. Conversely, show that if $\| \cdot \|$ is an arbitrary norm on $\mathbb{R}^d$ then there exists a symmetric convex body $B$ such that $\| \cdot \| = \| \cdot \|_B$.

https://doi.org/10.1017/9781108652865.004 Published online by Cambridge University Press